

IN THE CLAIMS

1. (Currently Amended) A method ~~of obscuring cryptographic computations~~ comprising:
performing modular exponentiation in a cryptographic computation such that memory accesses are independent of the numerical value of the exponent, wherein performing modular exponentiation is to comprise replacing a conditional multiplication operation with an unconditional multiplication operation and the unconditional multiplication operation is to be based on an obscuring factor; and
determining the obscuring factor for each bit of the exponent by adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity comprising a message minus one.

2-4. (Canceled)

5. (Original) The method of claim 1, wherein the exponent comprises at least one of a signature exponent and a decryption exponent in a RSA cryptographic system, and the cryptographic computation is at least one of signature and decryption.

6. (Original) The method of claim 5, wherein the cryptographic computation comprises $c^d \bmod n$, wherein c comprises a ciphertext message, d comprises the decryption exponent, and n comprises a modulus that is a product of two prime numbers.

7. (Original) The method of claim 1, wherein the modular exponentiation is performed as part of a Diffie-Hellman key exchange process.

8. (Original) The method of claim 1, wherein the modular exponentiation is performed as part of a Digital Signature Algorithm (DSA) process.

9. (Original) The method of claim 1, further comprising applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of a message from a memory, where v is the size of a window into the exponent's bits.

10. (Currently Amended) A method ~~of obscuring cryptographic computations by performing modular exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the exponent bit pattern~~ comprising:

setting an intermediate value to a message; and

for each bit i in the exponent, setting the intermediate value to the intermediate value multiplied by the intermediate value mod a modulus, wherein the modulus comprises a product

of two prime numbers, determining a current obscuring factor using the i 'th bit of the exponent, and setting the intermediate value to the intermediate value multiplied by the current obscuring factor mod the modulus, wherein determining the current obscuring factor comprises determining the current obscuring factor by adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity comprising the message minus one.

11. (Canceled)

12. (Original) The method of claim 10, wherein the exponent comprises at least one of a signature exponent and a decryption exponent in a RSA cryptographic system, and the cryptographic computation is at least one of signature and decryption.

13. (Original) The method of claim 10, further comprising applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of the message from a memory, where v is the size of a window into the exponent's bits.

14. – 23. (Canceled)

24. (Currently Amended) An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for obscuring cryptographic computations by performing modular exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the numerical value of the exponent, wherein a current obscuring factor is to be determined by adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity to comprise a message minus one.

25. (Original) The article of claim 24, wherein performing modular exponentiation comprises replacing a conditional multiplication operation with an unconditional multiplication operation.

26. (Original) The article of claim 24, further comprising instructions for applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of a message from a memory, where v is the size of a window into the exponent's bits.

27. (Currently Amended) An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for obscuring cryptographic computations by performing modular

exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the exponent bit pattern, the instructions causing

setting an intermediate value to a message; and

for each bit i in the exponent, setting the intermediate value to the intermediate value multiplied by the intermediate value mod a modulus, wherein the modulus comprises a product of two prime numbers, determining a current obscuring factor using the i 'th bit of the exponent, and setting the intermediate value to the intermediate value multiplied by the current obscuring factor mod the modulus, wherein determining the current obscuring factor is to comprise adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity to comprise the message minus one.

28. (Canceled)

29. (Original) The article of claim 27, wherein the exponent comprises at least one of a signature exponent and a decryption exponent in a RSA cryptographic system, and the cryptographic computation is at least one of signature and decryption.

30. (Original) The article of claim 27, further comprising instructions for applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of a message from a memory, where v is the size of a window into the exponent's bits.

31. – 32. (Canceled)